



JOHN NAIMO
AUDITOR-CONTROLLER

**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

August 18, 2016

TO: Supervisor Hilda L. Solis, Chair
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: John Naimo
Auditor-Controller

SUBJECT: **ANNUAL HEALTH INSURANCE PORTABILITY AND
ACCOUNTABILITY ACT PRIVACY RULE PROGRAM REPORT**

This report provides an annual update on the County's Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Program (Program). The Office of the Chief HIPAA Privacy Officer (CHPO) and associated responsibilities reside with the Auditor-Controller (A-C). This report includes: 1) ongoing implementation efforts; 2) modifications and new privacy-related regulations impacting the County's Program; 3) new and ongoing responsibilities imposed on covered departments; 4) annual breach reports provided to the U.S. Department of Health and Human Services (HHS); 5) audits completed by the CHPO in calendar year 2015; 6) HIPAA privacy complaints and investigations; 7) enforcement; 8) emerging trends; and 9) next steps.

Background

The HIPAA Privacy Rule¹ (Rule) establishes minimum federal standards for protecting the privacy of individually identifiable health information. The Rule confers certain rights on individuals, including accessing and amending their health information and obtaining a record of when and why their protected health information (PHI) has been shared with others for certain purposes. Covered entities and business associates may not use or disclose PHI, except as allowed by the Rule or with written authorization of the subject individual. The HIPAA Breach Notification Rule² requires HIPAA covered entities and

¹ 45 Code of Federal Regulations (CFR) Part 160 and Subparts A and E of Part 164

² 45 CFR Part 160 and Subparts A and D of Part 164

their business associates to provide notification following a breach of unsecured PHI.³ The CHPO's responsibilities are discussed below.

The CHPO continues to work with departments on an ongoing basis to implement changes to the Rule and related regulations. Additionally, programmatic and regulatory mandates require the CHPO to conduct ongoing audits, respond to reported breaches/incidents, investigate complaints, ensure departments are compliant with the Rule, and monitor workforce training. The departments, divisions, and commissions that are part of the County's Health Care Component and must comply with HIPAA are as follows:

- A-C's divisions and personnel who perform business associate functions as defined under the HIPAA regulations
- Chief Executive Office's (CEO) divisions and personnel who perform business associate functions
- Chief Information Office (HIPAA-related functions merged with the CEO in April 2016)
- County Counsel
- Executive Office of the Board of Supervisors, Human Immunodeficiency Virus (HIV) Commission
- Department of Health Services (DHS)
- Department of Human Resources' Employee Flexible Spending Accounts within the Employee Benefits Division
- Internal Services Department's (ISD) divisions and personnel who perform business associate functions
- Department of Mental Health (DMH)
- Probation Department – Probation Electronic Medical Record System
- Department of Public Health (DPH)
- Treasurer and Tax Collector's divisions and personnel who perform business associate functions

In addition to the departments listed above, County Counsel is currently reviewing the Emergency Medical Services' operations of the Fire Department to determine whether they should be included in the County's Health Care Component. At the very least, the Fire Department has engaged the expertise of the CHPO to develop a program that is sensitive to federal confidentiality laws.

³ Unsecured PHI is any PHI that is not rendered or determined to be unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology.

1. ONGOING IMPLEMENTATION EFFORTS

On January 17, 2013, the Office for Civil Rights (OCR) of HHS issued the Omnibus Final Rule⁴ implementing changes in regulations under HIPAA pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act. The changes were extensive and significantly strengthen privacy protections for patient health information while enhancing HHS' ability to enforce such protections. The Omnibus Final Rule was effective on March 26, 2013, with a compliance date for most provisions of September 23, 2013. HHS continues to update information regarding guidance for covered entities to be compliant with HIPAA and the HITECH Act.

While covered departments implemented and incorporated the changes into their HIPAA programs by HHS' deadline, we continue to work with them to ensure ongoing compliance with the regulations. Challenges for departments include information sharing projects involving PHI, implementing role-based training for staff, developing and rolling out policies and procedures across multiple facilities, complying with various and sometimes overlapping regulatory requirements, and ensuring that contracts and business associate agreements include adequate safeguards related to ongoing compliance with the regulations. As discussed below, HIPAA violations involving criminal actions are increasing. The CHPO works closely with County Counsel to assist covered departments with the Rule's implementation and compliance challenges.

2. MODIFICATIONS AND PRIVACY-RELATED REGULATIONS IMPACTING THE PROGRAM

When the HIPAA regulations were originally enacted, only covered entities were required to adhere to the law. That left many agencies with access to PHI, such as billing agencies, information technology companies, and labs outside the scope and jurisdiction of HIPAA. Although covered entities were required to enter into agreements with these business associates to whom they provided medical information, HHS did not have jurisdiction to enforce or penalize business associates for non-compliance with HIPAA regulations.

To address the enforcement gap, HIPAA was amended so business associates (including County departments that perform business associate functions) are now directly liable for HIPAA requirements related to safeguarding PHI and breach notification. Further, business associate functioning departments are now part of the County's Health Care Component, whereas prior to the HITECH Act those departments had a memorandum of understanding with the covered departments.

⁴ 45 CFR Parts 160 and 164

Omnibus Final Rule Implementation of Business Associate Functions and Agreements

The regulations require a business associate to contractually agree to implement administrative, physical, and technical safeguards to protect PHI. The Omnibus Final Rule expanded the definition of business associate to also include downstream subcontractors of business associates, and imposed direct liability on business associates and downstream vendors for violations of certain provisions, with maximum civil fines of up to \$1.5 million per violation per year. The CHPO and County Counsel worked with covered departments to ensure that business associate agreements were amended to include the updated HIPAA language. In addition, ISD's master agreements now include the updated HIPAA language.

HIPAA/HITECH Act Privacy and Security Committee

To ensure a seamless implementation of the Omnibus Final Rule for the covered departments, the CHPO and Chief Information Security Officer (CISO) established a HIPAA/HITECH Act Privacy and Security Committee (Committee) consisting of representatives from each of the County's Health Care Component departments. County Counsel is also an active participant on the Committee, and provides updates on legal requirements impacting the Program and covered departments.

The Committee meets monthly to discuss changes in regulations, implementation and standard requirements, updates to privacy and security policies and procedures, enforcement, and proposed/upcoming laws and policies that may impact the covered departments' HIPAA programs.

3. NEW AND ONGOING RESPONSIBILITIES IMPOSED ON COVERED DEPARTMENTS

HIPAA Training Program

Covered entities must train workforce members on the HIPAA and HITECH Act regulations and related policies and procedures to the extent necessary and appropriate for employees to carry out their functions without violating the regulations. The HIPAA covered departments, with the exception of DHS, utilize the County's Learning Management System (LMS) to train their workforce members. DHS provides training through vendors, direct classroom instruction, and self-study guides. Approximately 35,000 County workforce members receive some form of HIPAA training each year, which includes updates and changes to the Rule's regulations and relevant departmental policies.

At this time, the LMS-HIPAA training program does not include State or other privacy laws that may also apply to departments, specifically DHS. Thus, each department

must develop training material that informs their employees about these additional privacy laws applicable to their operations. The CHPO provides assistance, guidance, and approves the departments' HIPAA training programs to the extent they include the Rule's content. County Counsel is also part of the review and approval process.

4. ANNUAL BREACH REPORTS PROVIDED TO HHS

The HITECH Act created a federal notification of breach requirement for HIPAA covered entities and their business associates. Covered entities that otherwise hold, use, or disclose unsecured PHI must notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been accessed, acquired, or disclosed as a result of a breach. A covered entity's business associate is required to notify the covered entity of such breach by the business associate. The CHPO is the contact person for such notices by business associates.

Secondly, the federal Breach Notification Rule mandates that breaches of unsecured PHI be reported to HHS on an annual basis and to impacted individuals within 60 days of the covered entity's or business associate's discovery of a breach. If a breach of unsecured PHI impacts 500 or more individuals, covered entities must provide notice to both HHS and the impacted individuals without delay, but within 60 days of its discovery. There are exceptions, such as law enforcement may request that a covered entity delay notice to impacted individuals.

Annual reports are due to HHS by March 1st for those breaches that impacted fewer than 500 individuals and occurred in the previous calendar year. For the calendar year 2015, the County reported a total of 20 breaches to HHS, two of which were by business associates of the County. In comparison, a total of 28 breaches were reported to HHS for 2014. The decrease is attributable in part to ongoing outreach to the covered departments about HIPAA and the diligent application of privacy controls over patient and client data.

5. AUDITS COMPLETED IN CALENDAR YEAR 2015

A key responsibility of the CHPO is to conduct audits and reviews to ensure that the covered departments, which are part of the County's Health Care Component, are complying with the Rule. For calendar year 2015, the following programs were reviewed:

- DMH: Rio Hondo Mental Health Center follow-up review
- DPH: Substance Abuse Prevention Control Programs (SAPC), which included 11 SAPC Programs: Adult Treatment Recovery Services, Community Information Systems, Criminal Justice Unit, Drug Medi-Cal Adult Compliance and Technical Assistance, Contract Services Division, Adult Treatment and Recovery Services-Family Services, Office of Prevention and Youth Treatment Programs

and Policy, Community Assessment Service Centers, Drug Medi-Cal Billing System, Driving Under the Influence Program, and Informatics Resources/Web Applications

- DHS: Wilmington Health Center
- DHS: Health Services Administration HIPAA Training Program

The CHPO also conducts unannounced site visits to ensure that County clinics and hospitals are posting their notices of privacy practices according to HIPAA standards, and meeting other observable privacy program requirements. In calendar year 2015, the A-C's HIPAA Compliance Unit (HCU) visited 22 facilities, of which six were found to not be in full compliance with the HIPAA standards.

If there is a finding that a facility or program is not in compliance with the regulations or standards, the CHPO coordinates with the department's designated privacy and/or compliance officers in the development of a corrective action plan. Follow-up continues until all issues are adequately resolved.

6. HIPAA PRIVACY COMPLAINTS AND INVESTIGATIONS

HIPAA requires covered entities to establish a process for individuals to complain if they believe their privacy rights have been violated. Further, there must be a process to document complaints, allegations, breaches, and queries by anyone including constituents, patients, agencies, workforce members, and OCR. Complaints are received by the CHPO through the HIPAA Hotline (213) 974-2164, a dedicated HIPAA e-mail address (hipaa@auditor.lacounty.gov), in-person, and by mail. Covered departments also maintain a log of complaints that are reported to the CHPO on a quarterly basis.

For calendar year 2015, the CHPO's office logged 87 complaints, representing a 15% increase from 2014, when 72 complaints were received. Complaints and issues were resolved, and reported accordingly or pending action from another agency, such as HHS. The most common complaints against the County involved allegations of wrongful disclosure of PHI and County employees accessing medical records without a business need. The most common incidents that were reported by departments to the CHPO involved the loss/theft of computer devices, or loss of paper files that contain PHI.

7. ENFORCEMENT AND PENALTIES FOR NON-COMPLIANCE

HHS enforces HIPAA and the HITECH Act and may issue fines and penalties up to \$1.5 million per incident. HHS considers a number of factors in deciding whether to issue fines and penalties for a breach, including the adequacy of the covered entity's compliance infrastructure. To date, despite several reportable breaches and investigations by HHS, no penalties have been issued by HHS against the County.

8. EMERGING TRENDS

The scope and responsibilities of the CHPO were significantly increased with the initial passage of the HITECH Act in 2009 and became final in 2013. The HITECH Act established the Breach Notification Rule, which requires timely breach reporting to impacted individuals and HHS. When a large privacy breach is suspected, the CHPO, HCU, County Counsel, and impacted departmental staff must respond immediately to comply with the regulations and mitigate any harm to individuals and the County. When criminal activity is suspected, law enforcement agencies become an important component of the investigation and mitigation efforts. The County's largest breaches have been due to criminal activity, and the A-C's Office of County Investigations (OCI) and other law enforcement agencies, such as the District Attorney's (DA) Cyber Investigation Response Team, have provided resources to respond to these incidents.

For calendar year 2015, the CHPO logged ten criminal incidents concerning PHI. OCI and CHPO work with the DA, County Counsel, CISO, and other involved departments on the County's response to any theft of our clients' or employees' PHI, and provide support to other law enforcement agencies in their investigations. This immediate and in-depth response to breaches involving a criminal component has had a notable impact on our changing roles to meet the demands of an investigation while maintaining compliance with HIPAA, federal, and State breach notification regulations.

9. NEXT STEPS

The CHPO and the Committee have drafted proposed Board of Supervisors' (Board) HIPAA policies to address consistent and minimum standards for covered departments and their workforce members. The proposed draft policies include, requirements for employee HIPAA training, safeguarding PHI, and sanctions for workforce members who do not comply with the Rule. While we acknowledge that the covered departments have HIPAA policies that provide these requirements, Countywide policies establish a baseline throughout the organization and bring focus to key HIPAA requirements. We anticipate submitting these proposed policies to your Board for approval in late 2016 or early 2017, depending on the next phase of reviews.

Summary and Conclusion

The CHPO continues to advance awareness of health privacy matters through leadership of the Committee, ongoing training, audits, and by providing technical assistance and expertise to covered departments. The CHPO is responsive to departments, constituents, workforce members, business associates, privacy and information security officers, HHS, and your Board in resolving privacy complaints and concerns. The CHPO will continue to work with the covered departments to implement future changes to the regulations and to identify and address compliance issues and public complaints.

If you have any questions, please call me or your staff may contact Linda McBride, CHPO, at (213) 974-2166.

JN:AB:PH:RGC:LTM

c: Sachi A. Hamai, Chief Executive Officer
Jim McDonnell, Sheriff
Jackie Lacey, District Attorney
Lori Glasgow, Executive Officer, Board of Supervisors
Mary C. Wickham, County Counsel
Mitchell H. Katz, M.D., Director, Los Angeles County Health Agency
Cynthia A. Harding, M.P.H., Interim Director, Department of Public Health
Robin Kay, Ph.D., Acting Director, Department of Mental Health
Calvin C. Remington, Interim Chief Probation Officer
Lisa M. Garrett, Director of Personnel, Department of Human Resources
Dave Chittenden, Chief Deputy Director, Internal Services Department
Joseph Kelly, Treasurer and Tax Collector
Daryl L. Osby, Fire Chief, Fire Department